US Army Corps
of Engineers

DISTRICT SECURITY OFFICER (dSO) MANUAL

Electronic Signature System

Version 2.0

November 1, 1996

CEFMS

Corps of Engineers Financial Management System

FOREWORD

The CEFMS district security officer (dSO) capability is limited to Government employees. A designated dSO must read and understand this document. Refer to Appendix A for the signature requirement acknowledging that you have read and understand the dSO's responsibilities.

DISTRICT SECURITY OFFICER (dSO) MANUAL

TABLE OF CONTENTS

PAGE

SECTION 1.0 GENERAL 1-1
1.1 Purpose 1-1
1.2 Conventions Used in This Document 1-1
1.3 Background 1-1
1.4 COE District Level Functions 1-2
1.5 District Security Officer (dSO) Security Procedures 1-3
1.5.1 Designation of dSOs and Responsibilities 1-3
1.5.2 Smartcard and PIN Usage 1-4
1.5.3 Security of the Smartcard and PIN 1-5
1.5.4 Lost Smartcard or Compromised PIN 1-5
1.5.5 Security Violations - What Should You Report? 1-5

SECTION 2.0 ELECTRONIC SIGNATURE SYSTEM SITE REQUIREMENTS 2-1
2.1 District Security Officer (dSO) 2-1
2.2 Smartcard Approvers 2-1
2.3 Security Administrators (SAs) 2-1
2.4 Users 2-2
2.5 Technical Implementation Team 2-2
2.6 Hardware/Software Requirements 2-2
2.7 Instructions for Exporting ARGUS 300 2-2

SECTION 3.0 ELECTRONIC SIGNATURE INSTALLATION 3-1
3.1 Installing Electronic Signature Hardware and Software 3-1
3.1.1 Installing Electronic Signature Hardware 3-1
3.1.2 Installing Electronic Signature Software 3-3
3.2 Configuring VistaCom 3-4
3.3 Connecting to CEFMS 3-5

SECTION 4.0 ELECTRONIC SIGNATURE MAINTENANCE . . . . . OPERATIONS 4-1
4.1 Electronic Signature Menu Processing 4-1
4.1.1 Menu Selection 3 - Request Smartcards 4-1

DISTRICT SECURITY OFFICER (dSO) MANUAL

TABLE OF CONTENTS (Cont.)

		PAGE
4.1.2	Menu Selection 4 - Approve/Reject Smartcard Requests	4-2
4.1.3	Menu Selection 5 - Unlock User Smartcard	4-3
4.1.4	Menu Selection 6 - Log Off SA Smartcard	4-3
4.1.5	Menu Selection 7 - dSO Functions	4-4
4.1.5.1	Smartcard Types View Screen	4-4
4.1.5.2	Smartcard Status Values View Screen	4-5
4.1.5.3	Log New Smartcards	4-5
4.1.5.4	View Smartcard Information	4-6
4.1.5.5	Assign Smartcards	4-7
4.1.5.6	Unassign Smartcards	4-7
4.1.5.7	Activate Smartcards	4-7
4.1.5.7.1	Issuing Smartcards	4-8
4.1.5.7.2	Remote Assignment and Issuing of Smartcards	4-8
4.1.5.8	Deactivate Smartcards	4-9
4.1.5.9	Lost Smartcards	4-10
4.1.5.10	Unlock User Smartcard	4-10
4.1.5.11	Order Smartcards	4-11
4.1.5.12	Key Translation Center/ORACLE SID Setup	4-11
4.1.5.13	Key Translation Center/Card Request Setup	4-12
4.1.6	Menu Selection 8 - Execute dSO Startup Utility	4-12
4.2	Storage of Smartcards and PIN Envelopes	4-12
4.3	Error Messages	4-13

LIST OF APPENDICES

APPENDIX A	DSO ACKNOWLEDGEMENT FORM	A-1
B	REQUEST FOR ELECTRONIC SIGNATURE FORM (Smartcard Initialization)	B-1

1.0 GENERAL

1.1 Purpose. The purpose of this document is to provide instructions and procedures for the day-to-day operation of CEFMS Electronic Signature for Site Security Officers. A site is *defined as a physical location where a Security Officer is needed to perform these functions. This could be a division, district, field office or laboratory. Operational procedures described in this document were developed based on published standards and specifications, and by Government Accounting Office (GAO) and National Institute of Standards and Technology (NIST) guidelines.

1.2 Conventions Used In This Document. CEFMS is an Oracle based system. Oracle Forms/Screens is the main user interface to CEFMS. As such, when using forms that require the Electronic Signature screens, certain key stroke sequences have common functionality between screens. Key stroke sequences in this document are delimited by the '<', the less than character, and by the '>', the greater than character. For example, <ENTER> indicates that the Enter key, or as it is labeled on some keyboards, the Return key, should be depressed. As another example, <CTRL-F1> indicates that the 'control' key and the 'F1' key are depressed simultaneously. Listed below are some of the more common keys used by CEFMS.

KEY SEQUENCE	FUNCTION
<F2>	Retrieve and display all records without qualification
<F3>	Retrieve and display all records matching entered fields
<END>	Commit entered data to the database
<F10>	Exit the form screen
<PgDn>	Go to a screen giving more details about data
<ENTER>	Different meanings; commonly used to return from a detail screen to previous screen.

In addition, prompts will sometime appear on the screen, requesting that various smartcards be inserted into the smartcard reader to logon, enter a PIN or perform some action on a smartcard. Successful performance of Electronic Signature functions is dependent on successfully following instructional screen prompts.

1.3 Background. Electronic signature is the capability to "sign" a document electronically which eliminates the need for a "paper" signature. An electronic signature is not a pictorial, or graphic representation of a "paper" signature. An electronic signature electronically tags data with a Message Authentication Code (MAC). A mathematical algorithm, using information from smartcards and the data being MACed, creates a MAC. If, at some point, data changes that has been MACed, then the MAC will not verify, indicating that some or all of the data associated with a MAC has changed. A smartcard is similar in size, shape and substance to an ordinary

credit card. Unlike an ordinary credit card, the smartcard contains a microprocessor chip that actually stores data and performs calculations.

An Electronic Signature or MAC must meet several GAO requirements to be considered valid, including:

- € Two authorized users are required to generate a MAC (split knowledge/dual control)
- € The information contained on each users Smartcard must be unique to the user
- € The Smartcards are under the control of each individual Smartcard holder
- € The MAC is linked to the data being signed or MACed
- € The validity of the MAC can be determined at any point in time.

Within the Corps of Engineers (COE), the majority of smartcards used will be of two types: Security Administrator (SA) and User. An SA card should be assigned to an individual who has authority over a group of individuals that will sign documents in the normal course of their daily work. Each individual in that group is assigned a User card. Before a MAC may be generated, the SA must logon to each individual PC with his SA card. Each user will in turn logon to their PCs with their User card. This enforces a principal known as "split knowledge and dual control". What has been described to this point is normal operations for those using CEFMS and Electronic Signature.

1.4 COE District Level Functions. A COE District, for the purposes of this document, is defined as a District that has its own CEFMS database and operates somewhat autonomously. Each district will require several personnel to perform necessary Electronic Signature functions. These functions include:

- € Installing Electronic Signature hardware and software
- € Requesting Electronic Signature smartcards
- € Storing Electronic Signature smartcards and the accompanying PIN envelopes
- € Logging smartcards into CEFMS
- € Unlocking smartcards
- € Assigning and activating smartcards
- € Issuing smartcards and PIN envelopes
- € Assisting Electronic Signature Users.

From an Electronic Signature view point, the function that will be performed the most is the issuing of smartcards to CEFMS users. The typical sequence of events in the life of a smartcard are as follows:

1. A CEFMS user that does not have a smartcard, but requires a smartcard, makes a request for a smartcard.

2. The request is approved or disapproved by a CEFMS user with smartcard request approval/disapproval authority.
3. District Security Officers (dSOs) associate or assign a smartcard to the approved requester.
4. The CEFMS user receives smartcard and PIN:

    a) The dSOs activate the smartcard and physically give the smartcard to the user. Then the user is given an envelope containing the PIN for the smartcard. The envelope must be signed and the top portion of the envelope retained by the dSO.

    or

    b) The dSO_1 mails the smartcard to the User. Upon receipt, the user notifies the dSOs. Based on this notification, the dSO_2 will mail the PIN envelope to the user. Upon receipt of the PIN envelope, the user will observe for tempering and then sign. The user will return the top portion to the dSO. Upon notification that the user has received the PIN, the dSOs will activate the card.

5. The smartcard is used.
6. After the smartcard's lifetime is over, the smartcard must be deactivated by the dSO.
7. The smartcard is reused.

1.5 District Security Officer (dSO) Security Procedures.

1.5.1 Designation of dSOs and Responsibilities.

a. Each Corps of Engineers Financial Management System (CEFMS) site will have two primary dSOs designated dSO1 and dSO2 to perform Electronic Signature management functions for smartcards. The dSO1 and dSO2 must have at least one backup (but no more than two) to perform their same functions. The backups are designated dSOb1 and dSOb2. **If a primary dSO and backup are both absent, Electronic Signature functions can not be performed.**

(1) DSO1 (and dSOb1) will be responsible for the security and issuing of User smartcards and Security Administrator (SA) Personal Identification Number (PIN) envelopes.

(2) DSO2 (and dSOb2) will be responsible for the security and issuing of SA smartcards and User PIN envelopes.

b. Each dSO and backup will have a UNIX user ID and password and will be granted privileges by the CEFMS DataBase Administrator (DBA) to perform dSO functions. These functions will be set in the CEFMS Access Control Table.

c. The dSOs for each site will be designated to the regional centers by memorandum signed by the Commander. This memorandum will include the dSO type (dSO1 or dSO2), name, phone number, address, and dSO designation (primary or backup). Any changes to the dSO list must also be by memorandum to the regional centers. The address for CPC is:

U.S. Army Engineer Waterways Experiment Station
Attn: CEWES-IM-C/David T. Turner
3909 Halls Ferry Road
Vicksburg, MS 39180-6199

The address for WPC is:

USA Engineer District, Portland
Western Processing Center
Attn: CENPP-IM-P (Sandra Smith/Randy Lujan)
PO Box 2946
Portland, OR 97208-2946

Additionally, one copy of the memorandum must be sent to the CEFMS office:

USACE Finance Center
Financial Systems Development, Maintenance
& Training (CEFC-AS)
Attn: Teresa Brown
4801 University Square, Suite 1
Huntsville, AL 35816

The central security officers at the regional centers will not issue a dSO card to anyone who is not on the list (resulting from the memorandum). Card requests and mailing of cards and PINs will only be made to dSOs on the list.

d. DSOs must be government employees, and given training in the operating procedures and security requirements for Electronic Signatures before performing dSO functions.

e. Smartcard Holders will be Government employees. DSOs will verify an individual's status before assigning, activating, or issuing a Smartcard. If unsure, dSOs will contact the Security Office.

1.5.2 Smartcard and PIN Usage. Your dSO is logged on when entering the dSO CEFMS Menu and logged off with a normal termination. **DO NOT LEAVE THE COMPUTER UNTIL YOU HAVE COMPLETED YOUR SESSION.**

1.5.3 Security of the Smartcard and PIN. Memorize your PIN. DO NOT write it down (especially on the smartcard) or share with others.

a. When not in use, keep your smartcard in your possession, preferably a wallet or purse, or in a locked cabinet, drawer, or container accessible only by you. DO NOT LEAVE YOUR WALLET OR PURSE UNSECURED OR UNATTENDED BY YOU.

b. If you retire, transfer, or leave the organization, you must notify the dSOs, return your smartcard to them for deactivation, and sign a Log Sheet for Deactivated Smartcards.

c. Think of your smartcard as a personal credit card or blank check. The Electronic Signature generated by the smartcard is your signature. If another person uses it, you will bear the consequences.

1.5.4 Lost Smartcard or Compromised PIN. A lost smartcard or compromised PIN is a serious security issue. You can be held responsible for transactions authorized with the missing or compromised card.

a. If your PIN is revealed to someone else or you suspect it has been compromised, contact a dSO immediately for a new smartcard. Take the smartcard to the dSOs for deactivation and sign the Log Sheet for Deactivated Smartcards. Messages previously "signed" by you may still be verified.

b. If your smartcard is lost/stolen, contact a dSO immediately for deactivation. You must go to the dSOs to obtain a new smartcard and PIN and sign a Log Sheet for Lost/Stolen Smartcards. Signatures generated by the lost/stolen smartcard after the deactivation date may not be verified.

1.5.5 Security Violations - What Should You Report? In addition to the security requirements in the preceding paragraphs, report the following violations to the Security Office.

a. If you see or know of unauthorized use of smartcards or PINs, i.e., sharing, notify the individual's supervisor for appropriate disciplinary action.

b. If you find an unattended computer with a smartcard in the smartcard reader, attempt to log them off CEFMS and remove the smartcard. If you cannot log them off, remove the smartcard and take to the individual's supervisor. Inform the supervisor of the incident so that he/she may take appropriate disciplinary action.

c. If you find a smartcard, take it to your supervisor so he/she may decide if disciplinary action is necessary. The user may have already reported the loss of the smartcard to a dSO.

d. If you find a PIN written down, notify the supervisor for appropriate disciplinary action. PINs should be memorized and not written down for unauthorized viewing.

2.0 ELECTRONIC SIGNATURE SYSTEM SITE REQUIREMENTS

2.1 District Security Officer (dSO). Each site with a CEFMS database must appoint two dSOs and backups for each. **Each site should have no more than 2 backups for each dso.** The dSOs will have responsibility for the following:

- € shipping smartcards to the regional key management center
- € logging smartcards when received, securely storing smartcards and PIN envelopes
- € assigning/issuing smartcards and PIN envelopes to users
- € assisting users with electronic signature questions/problems.

The dSOs will have separate responsibilities: dSO1 will be responsible for User cards and SA PIN envelopes and dSO2 will be responsible for SA cards and User PIN envelopes. Each backup will have the same responsibility as the primary.

The dSO must have a user ID for CEFMS and be authorized in the Access Control Table to perform dSO functions. The dSO will receive his own smartcard and pin envelope from the central security officers. The dSO will assign his own smartcard through the CEFMS screens; and will approve, assign and issue the first two cards requested for the Smartcard Approvers. One card must be for an SA and the second card must be for a User in order to begin the process of issuing cards.

2.2 Smartcard Approvers. Each CEFMS database site must appoint a Smartcard Approver(s) to be responsible for approving a smartcard request from users and SAs. The Smartcard Approver must have a CEFMS user ID/password and be assigned authority in access control to approve smartcard requests.

The Smartcard Approver must have a smartcard in order to electronically approve smartcard requests. The initial smartcard requests for an SA card and a User card must be approved by the dSOs.

2.3 Security Administrators (SAs). SAs must be appointed to logon to the electronic signature hardware on each PC before the users. Once an SA logons, the SA information stays on the security adapter. An SA must invoke the shutdown function from the CEFMS Electronic Signature Menu, periodically, before leaving or retiring from a position or if the SA loses the electronic signature card. The shutdown function removes the SA information from the security adapter, thus requiring that an SA logon again the next time Electronic Signature functions are used. In the area of disbursing, SA's must logon and shutdown on a daily basis. It is recommended that SAs be assigned for each organization due to the re-initialization that is required when an SA leaves, retires or loses a card.

The SAs must have a CEFMS user ID/password. They must request a SA smartcard using the CEFMS screens for Electronic Signature. This request must be approved by an appointed Smartcard Approver.

SAs may use their smartcards to sign documents as Users; however, if the SA role is a User, he must have another SA logon to the Electronic Signature hardware.

2.4 Users. Any site personnel required to sign documents in CEFMS may request a smartcard in CEFMS. The user must first have a CEFMS user ID/password in order to request a smartcard using the CEFMS screens.

If a user is also an SA, he only needs to request a SA card. Any request must be approved by an appointed Smartcard Approver.

2.5 Technical Implementation Team. A team should be appointed with the technical ability to install the electronic signature hardware and software on each PC requiring the electronic signature functionality.

2.6 Hardware/Software Requirements. The following items are required to install/implement electronic signatures:

- € CEFMS database
- € Cryptographic PC adapter board (Argus 300)
- € Smartcard reader
- € ESIGISR software
- € Vistacom Product (VISTACOM 5.2 release 3.2 with modified VCSMGR (ESIGMGR))
- € Initialized smartcards
- € PIN for the smartcards.

2.7 Instructions for Exporting ARGUS 300.

In order to export the **ARGUS 300,** the following documentation must be completed and submitted to the Department of State.

- € Prepare a letter for exemption from registration with the Department of State required by ***ITAR 22 CFR 120-130***. The exemption is based on 122.1B1, officers and employees acting in official capacity of the US Government.

- € Prepare form **DSP-5** for each shipping address and each shipment made to that address. The forms can be requested by fax from Donna Davis at the State Department, 703-875-6647(facsimile number).

- € Prepare a list of freight forwarders for each shipment (2 copies).

- € Prepare a letter stating the reason the items are needed by the foreign end user (7 copies).

- € Submit Technical Information regarding the**ARGUS**. Litronics should be able to provide a technical sheet on the product. (7 copies).

- € Call the State Department at 703-812-2406 if you have any questions regarding the required documentation. Point of contacts (POCs) are Darlene Staniszowski and Kathy Niedringhaus. Please mention that you are wanting to export encryption hardware. The POCs are not familiar with the details of our electronic system.

3.0 ELECTRONIC SIGNATURE INSTALLATION

3.1 Installing Electronic Signature Hardware and Software. The following steps must be accomplished to use Electronic Signature in CEFMS. Each PC to be used to perform Electronic Signature functions in CEFMS must have the Electronic Signature hardware and software installed. Each individual user must use an electronic signature equipped PC as a terminal to connect to a CEFMS hardware platform which will, in most cases, be a SUN SPARC series computer. The PC must use the VistaCom Terminal Emulator software package for DOS that has been modified for use with CEFMS and must be configured to use the Corps 220 terminal emulation. CEFMS may only be accessed using Telnet terminal sessions.

3.1.1 Installing Electronic Signature Hardware. A Security Adapter printed circuit board must be installed in all PCs that access Electronic Signature functions in CEFMS. Shown below are the steps necessary to install a Security Adapter printed circuit board.

STEP 1:

DIP switch 2 sets the base I/O address of the Security Adapter. The DIP switch consists of 6 switches. Only the first five are valid. The setting of the last switch is irrelevant. Insure that the first five switches on DIP switch 2, labeled as SW2 on the Security Adapter, are set as shown:

```
ON   OFF   ON   ON   OFF
 1    2     3    4    5
```

With DIP switch 2 set as shown the I/O address is 250h, the factory default.

STEP 2:

The address of the mapping point of the EPROM located on the Security Adapter into computer memory must be set using DIP switch 1. Labeled as SW1 on the Security Adapter, consists of 6 switches, all of which are valid. Set DIP switch 1 as shown:

```
ON   OFF   OFF   ON   OFF   OFF
 1    2     3    4    5     6
```

With DIP switch 1 set as shown, the EPROM address is D8000h, the factory default. Please note that the EPROM address and the base I/O address must be set to a valid combination or the Electronic Signature software will not function. The table shown below displays all the valid EPROM and base I/O address combinations and the corresponding switch settings. Note that a '0' corresponds to a switch setting of "ON" and a '1' corresponds to a switch setting of "OFF".

All addresses are in hexadecimal.

EPROM ADDRESS	SW1 123456	BASE I/O ADDRESS	SW2 12345
C8000	010011	250	01001
CC000	110011	270	11001
D0000	001011	210	00001
D4000	101011	230	10001
D8000	011011	250	01001 (FACTORY DEFAULT)
DC000	111011	270	11001
E0000	000111	310	00011
E4000	100111	330	10011
E8000	010111	350	01011
EC000	110111	370	11011

IMPORTANT: EPROM and I/O addresses must be set to one of the combinations shown in the table. For example, if an EPROM address of E4000h is selected then the I/O address must be set to 330h.

STEP 3:

Insert the Security Adapter into any available 8 or 16 Bit ISA bus slot.

STEP 4:

Plug the connector on the end of the card reader cord into the matching connector on the rear of the Security Adapter.

STEP 5:

A keyboard intercept cable is included with the Security Adapter. There are two types of cables available: one for standard PC keyboards that have a DIN 5 connector, and one for PS/2 style keyboards that have a mini DIN 6 connector. With either keyboard intercept cable there is a mini DIN 6 connector on one end that must be plugged into the matching connector on the security adapter. The other end of the keyboard intercept cable has a double ended connector: a male and female DIN 5 connector for standard PCs or a male and female mini DIN 6 connector for PS/2 computers. Plug the male end of the double ended connector into the keyboard connector on the computer system. Then plug the connector on the end of the keyboard cable into the female end of the double ended connector on the keyboard intercept cable.

The type of keyboard intercept cable must be specified when ordering Security Adapters. Specify the keyboard intercept cable as standard or PS/2.

STEP 6:

Power on and boot the computer. During the boot process, after the machine BIOS memory check, the message "Litronic ARGUS/300 installed at xxxxx", where "xxxxx" is the EPROM address that the Security Adapter is set. If this message fails to display or if the computer locks up during the boot process, chances are good that an address conflict exists. Try a different address. If all possible address combinations on the Security Adapter are tried and do not correct the problem, a shadowing or memory manager relocation problem may exist. First, check to see that shadowing for the EPROM address of the Security Adapter has been disabled. This is most often done by using the BIOS setup utility for the computer. If a memory manager is in use, the memory manager may be trying to relocate the code and data, beginning at the EPROM address that the Security Adapter is using to a location in upper or high memory. The Security Adapter will not function if that is done. The memory manager must be told to exclude relocating the code and data for the Security Adapter when the memory manager is started. This is done most often by the use of the memory manager command line option "exclude". Consult software documentation for the specific memory manager in use as to proper usage and syntax.

Important: The Security Adapter does not use a hardware interrupt, therefore, the Security Adapter cannot cause interrupt (IRQ) conflicts.

3.1.2 Installing Electronic Signature Software. Electronic Signature is software developed to specifically drive the Electronic Signature Security Adapter printed circuit board in a DOS environment while running the modified DOS VistaCom terminal emulation and communications software. This software must reside on the hard disk drive of each PC required to perform Electronic Signature functions. The steps necessary to install the Electronic Signature software drivers are shown below:

1. Insert the floppy disk containing the DOS Electronic Signature drivers into the appropriate (3.5 or 5.25) floppy drive on the PC.

2. Issue the following command at the DOS prompt:

   copy drive:*.exe c:\path

Where "drive" is the device name of the floppy drive device containing the electronic signature floppy disk, either "a" or "b", and where "path" is a directory, such as "c:\DOS", that is always in the DOS "PATH" variable.

3. Verify that two files, "esigisr.exe" and "esigmgr.exe", now reside on the hard drive.

4. Load the driver by typing "**esigisr**" at the DOS prompt and depressing the <ENTER> key. The driver will default to using software interrupt Ox66h. If there is a conflict, specify another interrupt on the command line when loading the driver. Interrupts Ox61h thru Ox67h may be used. To load the driver using interrupt Ox63h, the following syntax would be used:

   esigisr Ox63

   If the driver does not load, the message "Security board not installed, terminating!" will be displayed. Even if a Security Adapter is installed in the PC, it is still possible to get the message indicating a Security Adapter is not installed. This is most likely because of one or more of the following:

   - the I/O address of the Security Adapter conflicts with another board installed in the computer
   - the base BIOS address of the Security Adapter conflicts with another board installed in the computer
   - shadowing is enabled for the base BIOS (EPROM) address of the Security Adapter
   - a memory manager is trying to relocate the contents of memory located at the base BIOS (EPROM) address of the Security Adapter
   - a software interrupt conflict exists.

Paragraph 3.1.1 discusses the problems identified above and possible resolutions.

3.2 Configuring VistaCom. VistaCom must be specifically configured for use with CEFMS and Electronic Signature. Accessing CEFMS, whether or not Electronic Signature functions are used, **MUST** be performed as described. Only telnet sessions with CEFMS are supported. If a modem is to be used to communicate with a CEFMS platform, then SLIP or PPP protocol must be used. Direct modem or hardwired connections **should not** be used. Problems created by the use of direct modem or hardwired connections **cannot** be supported by the CEFMS development team. Shown below are the steps necessary to configure VistaCom, assuming that the VistaCom package is already loaded.

1. Enter VistaCom by issuing the "vcom" command at the DOS prompt.

2. Select "config" from the options at the bottom of the VistaCom screen.

3. Define the connection to the CEFMS platform to be used.

   € Select a connection type of "UNIX" from the choices that VistaCom supplies.

   € Enter an IP address or host synonym for the desired CEFMS platform connection. Baud Rate, data bits, etc., are not required for telnet connections. The connection method should be "telnet".

   € For all of the above described types of connections, enter a terminal emulator type of "CORPS220" in the Emulator field.

4. Save the connection definition using the VistaCom Menu selection at the bottom of the screen. While exiting "config", VistaCom will prompt for the connection name. Name the connection as desired.

5. Exit vcom.

6. Create a DOS batch file and locate the file in a directory in the DOS PATH variable. That file must contain the following:

vcon connection_name (where "connection name" is the name given in step 4)
esigmgr /noclear

vcon and esigmgr must reside in a directory in the DOS PATH variable.

3.3 Connecting To CEFMS. Before connecting to the CEFMS platform through a defined connection, esigisr must be loaded by typing "**esigisr**" at the DOS prompt and depressing the <ENTER> key. Esigisr is a "terminate and stay resident program". If it is necessary to unload esigisr, type "**esigisr /u**" at the DOS prompt and depress <ENTER>. It may be beneficial to load esigisr from the autoexec.bat file at boot time.

Connect to the CEFMS platform by invoking the batch file created in step 6 of Paragraph 3.2 by entering the name of the batch file at the DOS prompt and depressing <ENTER>. If VistaCOM and communications software have been installed correctly, a UNIX login prompt will be displayed momentarily. Login to the UNIX system and access CEFMS by typing **fms**" at the UNIX prompt and depressing <ENTER>. To use Electronic Signature, respond to prompts as they appear and perform the requested action. **DO NOT** remove an Electronic Signature User smartcard until a prompt appears stating that the user is being logged off. After that message is no longer displayed, the user card may be removed; otherwise, the card will be locked and unusable until unlocked.

This document **IS NOT** intended to describe how to install VistaCom or any communications software, such as PC/TCP network software for DOS. This document makes the presumption that VistaCom and all communications software have been installed previously and functions properly before attempting to use CEFMS and Electronic Signature. In addition, the Electronic Signature terminate and stay resident driver may cause some software not to execute because of the memory the driver uses. In those cases, it will be necessary to experiment with different "config.sys" and "autoexec.bat" configurations.

4.0 ELECTRONIC SIGNATURE MAINTENANCE OPERATIONS

4.1 Electronic Signature Menu Processing.

a. The CEFMS Main Menu is displayed by typing '**fms**" and depressing <ENTER> at the UNIX prompt after successfully logging on to the UNIX machine running CEFMS.

b. When entering the CEFMS system, a prompt will be displayed to logon an SA and USER. For those not performing functions requiring Electronic Signature or first time CEFMS users, simply depress the <ENTER> key to continue. An error message will be displayed stating that electronic signature capability is not available. That is normal and at this point should be ignored.

c. The Electronic Signature functions are accessed by selecting option "7" from the CEFMS Main Menu. The Electronic Signature Menu is then displayed and provides the following selections.

```
€€€€€€€€€ CORPS OF ENGINEERS ELECTRONIC SIGNATURE MENU € 1.56 €€€
€                                                              €
€                                                              €
€                    1 - EXIT FROM CEFMS                       €
€                    2 - PREVIOUS SCREEN                       €
€                    3 - REQUEST SMARTCARDS                    €
€                    4 - APPROVE/REJECT SMARTCARD REQUESTS     €
€                    5 - UNLOCK USER SMARTCARD                 €
€                    6 - LOG OFF SA SMARTCARD                  €
€                    7 - dSO FUNCTIONS                         €
€                    8 - EXECUTE dSO STARTUP UTILITY           €
€                                                              €
€                                                              €
€          Please Enter Selection:                             €
€                                                              €
€                                                              €
€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€
```

Options 3 through 8 are discussed in the following paragraphs.

4.1.1 Menu Selection 3 - Request Smartcards.

a. CEFMS Electronic Signature users utilize this selection to initially request a smartcard. When menu option "3" is selected, the '**REQUEST ELECTRONIC SIGNATURE**

SMARTCARD SCREEN" will be displayed. The <F9> key should be depressed to request a smartcard for the requestor. The requestor should then enter a "U" if requesting a User card, or an "S", if requesting an SA card. The <END> key should be depressed to commit the request. The <F10> key can then be depressed to exit the screen and return to the Electronic Signature menu. From there, menu selections can be made as desired either to access other CEFMS functions or to exit from CEFMS.

b. A user may request only one card and once issued, the user may not request a new card until (1) the old card is deactivated; (2) the card is to expire within 30 days or (3) the card is expired.

d. The type of card needed is determined by the requestor's supervisor.

e. When the request is committed, the request will then be put in a queue, electronically, to be reviewed by a designated approving official.

f. The status of the card request can be checked periodically by accessing this menu selection and depressing the <CTRL-F2> key sequence. Another screen will be displayed which shows whether the request has been acted on and whether the request was approved or disapproved. Nothing may be modified or entered on this screen. A return to the previous screen is required and may be performed by depressing the <ENTER> key.

4.1.2 Menu Selection 4 - Approve/Reject Smartcard Requests.

a. After a smartcard is requested, the request must be either approved or disapproved. This menu selection provides that capability.

b. Within each COE District, there must be personnel designated as "smartcard request approvers". Each person designated as a smartcard approver will be indicated as such in the CEFMS Access Control Table for that COE District. Access to this menu selection will be limited to personnel designated as smartcard approvers and successful login of an Electronic Signature SA and User. The approver may be an SA and login as a User, but another SA must login first.

c. When menu option "4" is selected, the "**APPROVE ELECTRONIC SIGNATURE SMARTCARD REQUEST SCREEN**" will be displayed. The screen will display all smartcard requests that have not been either approved or rejected.

d. If more than one screen of requests is pending, the arrow keys may be used to scroll up and down through the pending requests. The cursor will automatically be positioned in the "approved" field for each pending request as they are scrolled.

e. A request may be approved by entering "Y" or disapproved by entering "N" in the "approved" field.

f. When the approver is finished "approving" smartcard requests, the <END> key should be depressed to commit the requests. This will forward the requests to the dSOs who will issue cards and PIN envelopes.

g. Depressing the <F10> key will cause the screen to be exited and all approval actions discarded.

h. If the <PgDn> key is depressed, a screen is displayed giving detailed information about the request. Information on the detailed screen may not be modified, entered or deleted. Depressing the <ENTER> key will cause the original "**APPROVE/ELECTRONIC SIGNATURE SMARTCARD REQUEST SCREEN**" to be re-displayed.

i. Depressing the <F3> key will cause a query to be executed. Field values on either screen may be changed to values to query on; matching queries will be displayed and can be scrolled through using the arrow keys.

j. Depressing the <CTRL-F1> keys sequence will cause the list of pending smartcard requests to be displayed.

4.1.3 Menu Selection 5 - Unlock User Smartcard.

a. Menu option "5" allows users to unlock their own cards if the card was locked due to an improper log off when exiting from CEFMS.

b. The user will be prompted to insert his card and enter the correct PIN. If the correct PIN is entered, then the card will be unlocked.

c. This option will not unlock a card which was locked due to nine consecutive, unsuccessful attempts to enter the correct PIN. The dSOs must unlock cards which are locked due to entry of incorrect PIN.

4.1.4 Menu Selection 6 - Log Off SA Smartcard.

a. Menu option "6" allows any SA to log off the other SA used to initialize an ARGUS 300 electronic signature board. The user will be prompted to insert an SA card and enter the correct PIN.

b. In the areas of disbursing, this should be done on a daily basis; otherwise, this log off should occur when an SA leaves an organization and on a scheduled basis such as quarterly or when the PC is not scheduled for CEFMS use and access cannot be controlled.

4.1.5 Menu Selection 7 - dSO Functions.

a. Each COE District must have two dSOs and a backup for each. Two of the dSOs will be primary dSOs; the primary dSOs shall be designated as dSO1 and dSO2. Two of the dSOs will be backup dSOs; the backup dSOs shall be designated as dSOb1 and dSOb2.

b. Two dSOs are required to login with their respective smartcards on the same PC to perform dSO functions.

c. When menu option "7" is selected, a prompt requesting that dSO1 insert the dSO1 smartcard into the smartcard reader will be displayed. The dSO1 or dSOb1 should insert their smartcard and login by following directions displayed by the prompts. Similarly, the process must be repeated by either dSO2 or dSOb2.

d. After the two dSOs have successfully logged in with their smartcards, the following dSO Functions Menu is displayed:

```
€€€€€€€€€€€€ CORPS OF ENGINEERS dSO FUNCTIONS MENU €€€€ 1.57 €€€€
€                                                              €
€                   1 - EXIT FROM CEFMS                        €
€                   2 - PREVIOUS SCREEN                        €
€                                                              €
€    3 - SMARTCARD TYPES VIEW SCREEN    13 - ORDER SMARTCARDS   €
€    4 - SMARTCARD STATUS VALUES VIEW   14 - KEY TRANSLATION    €
€        SCREEN                              CENTER ORACLE     €
€    5 - LOG NEW SMARTCARDS                  SID SETUP         €
€    6 - VIEW SMARTCARD INFORMATION     15 - KEY TRANSLATION    €
€    7 - ASSIGN SMARTCARDS                   CENTER CARD       €
€    8 - UNASSIGN SMARTCARDS                 REQUEST SETUP     €
€    9 - ACTIVATE SMARTCARDS                                   €
€   10 - DEACTIVATE SMARTCARDS                                 €
€   11 - LOST SMARTCARDS                                       €
€   12 - UNLOCK USER SMARTCARD                                 €
€                                                              €
€                 Please Enter Selection:  2                   €
€                                                              €
€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€€
```

The following paragraphs describe options from the dSO Functions Menu.

4.1.5.1 Smartcard Types View Screen.

a. There are various types of smartcards, such as an SA or User smartcard. They physically appear the same, but are not equally created. This menu selection is used to view the valid types of smartcards in the CEFMS Electronic Signature System.

b. When menu option "3" is selected, the '**CARD TYPE VIEW SCREEN**" will be displayed. This screen lists the designators and descriptions for the currently recognizable smartcard types including:

D - District Security Officer (dSO)
S - System Administrator
U - User

c. It should be noted that any existing card type may not be removed or modified nor new smartcard types added by dSOs.

4.1.5.2 Smartcard Status Values View Screen.

a. A smartcard may have one and only one of several possible status, or status indicators.

b. When menu option "4" is selected, the '**CARD STATUS VIEW SCREEN**" will be displayed. This screen lists the status values or status indicators that a smartcard may have in the CEFMS Electronic Signature System including:

A - Available
B - Assigned
C - Activated
D - Archived
E - Retired
F - Lost

c. New status values may not be added nor existing status values removed or modified by dSOs.

4.1.5.3 Log New Smartcards.

a. When dSOs receive new smartcard supplies they must be logged into CEFMS before they may be issued. This does not mean that all smartcards must be logged in immediately. Small groups may be logged in as necessary, until all the smartcards have been logged in.

b. When menu option "5" is selected, the '**SECURITY OFFICER SMARTCARD LOG SCREEN**" will be displayed.

c. To begin logging smartcards, depress the <CTRL-F1> key sequence. A prompt will be displayed asking that a smartcard be inserted into the smartcard reader or "Q" entered to terminate the smartcard log function.

d. A previously unlogged smartcard should then be inserted into the smartcard reader. When a smartcard is inserted into the smartcard reader, information about the card is retrieved from the card itself and by network communications with the Central Key Translation Facility. As the information is retrieved, the dSOs will observe that the retrieved information is used to populate each of the fields associated with the smartcard on the screen. After the smartcard data is retrieved, a prompt will be displayed asking that the smartcard be removed from the smartcard reader. When the smartcard is removed, the original prompt asking for a smartcard to be inserted into the smartcard reader or enter "Q" to quit will be re-displayed. The process can then be repeated as desired.

e. To terminate the logging session, depress the "Q" key. At that point the cards just logged are committed to the CEFMS database.

4.1.5.4 View Smartcard Information.

a. This function permits the dSOs to view information on all smartcards logged in to their COE District's CEFMS database.

b. When menu option "6" is selected, the screen will clear and the "**SMARTCARD STATUS SCREEN**" will be displayed showing smartcard information on the first 15 smartcards in the database.

c. The information displayed for each smartcard includes:

- Serial number
- Card UID
- Card type
- Status
- Name of person the card is assigned

d. Depressing the <SHIFT-F2> keys causes information on the next 15 smartcards to be displayed. The <SHIFT-F2> keys can be repeatedly used to display information on all smartcards in the database.

e. If the display of information about a specific smartcard or group of smartcards is desired, standard Oracle query techniques may be used. All fields of the "SMARTCARD STATUS SCREEN" permit queries. Use the <TAB> or <ENTER> key to position the cursor in the field to be queried. Enter the data to be used in the query and depress the <F3> key to initiate the query. Information on smartcards that match the query will be displayed. If more than one screen full of matching smartcards is found, use the <SHIFT-F2> keys to display the next screen.

4.1.5.5 Assign Smartcards.

a. This function is used by the dSOs to associate or assign a specific smartcard with an individual.

b. When menu option "7" is selected, the '**DSO CARD ASSIGNMENT SCREEN**" will be displayed. This screen provides a list of approved smartcard requests awaiting assignment.

c. Smartcards must first be assigned and then activated.

d. When the cursor is positioned on the assignment request desired, enter 'Y' and then depress the <End> key to make the assignment. A prompt will appear requesting that a smartcard be inserted into the smartcard reader. A smartcard of the type requested must be inserted into the smartcard reader. For example, a request for an SA smartcard must be assigned using an available or newly logged in SA smartcard. Similarly, an available User card must be used.

e. When the dSOs have finished assigning smartcards, depressing the <END> key will commit the assignment requests to the CEFMS database, otherwise all assignments that have been performed will be lost, if not previously committed.

4.1.5.6 Unassign Smartcards.

a. This function is used by the dSOs to unassign a specific smartcard that has already been assigned to an individual.

b. When menu option "8" is selected, the '**DSO CARD UNASSIGNMENT SCREEN**" will be displayed.

c. Upon entering this screen a list of assigned smartcard/users will be displayed. When the cursor is positioned on the assigned entry, enter 'Y' then depress the <End> key to unassign the smartcard.

4.1.5.7 Activate Smartcards.

a. The dSO should activate smartcards only at the time they are physically received by a user. Activation may occur when a user is present to receive his smartcard or after acknowledgement from the remote requestor that the smartcard and PIN were separately received.

b. When menu option "9" is selected, the '**DSO CARD ACTIVATION SCREEN**" is displayed.

c. All smartcards awaiting activation will be displayed when selecting this option. The up/down arrow keys may be used to scroll through the entries.

d. The cursor should be positioned on the card to activate. Enter 'Y' then depress the <End> key to activate the card.

4.1.5.7.1 Issuing Smartcards.

If a user appears in person to receive a smartcard:

a. A valid driver license or Civilian ID card may be required to verify identification.

b. The individual will be given a copy of the Electronic Signature Users Guide. The user must read, sign, and date the Smartcard Holders Responsibilities Form before receiving a smartcard and PIN. A copy of the signed signature page will be provided to the user.

c. After verifying the person's identity, the dSOs will activate the smartcard and issue the smartcard and PIN to the employee.

- If the smartcard being issued is for a User, dSO1 will issue the smartcard and dSO2 will issue the User PIN envelope.

- If the smartcard being issued is for an SA, dSO2 will issue the smartcard and dSO1 will issue the SA PIN envelope.

d. The individual will check the PIN envelope to detect tampering. If none is found, the user will sign the top portion of the envelope, tear it off, and return to the issuing dSO. The dSO will file the signed top portion.

e. The bottom portion containing the smartcard holer's unique PIN (i.e., password) is kept by the individual.

4.1.5.7.2. Remote Assignment and Issuing of Smartcards.

If a user is remotely located and cannot receive his/her card in person:

a. If the smartcard request is approved by the Smartcard Approver, assign a smartcard through the DSO CARD ASSIGNMENT SCREEN.

b. The requestor should be mailed the smartcard by**Certified Mail - Return Receipt Requested**.

c. When the requestor receives the smartcard, he should sign for the Certified Mail and call the dSO to let him/her know the user received the smartcard. If a response is not received in a reasonable amount of time or if the smartcard is damaged or lost, the card should be unassigned and the PIN envelope destroyed. The user must be assigned a new card.

d. Upon confirmation that the user received the smartcard, the dSO will mail the PIN envelope by **Certified Mail - Return Receipt Requested**.

e. Upon receipt, the user must sign for the mail and examine the PIN envelope for tampering. If okay, the user will sign the top portion of the PIN envelope and tear it open.

f. The user must return the top portion of the PIN envelope to the issuing dSO by **U.S. Postal Service - Regular Mail, First Class**.

g. The user must call the issuing dSO to acknowledge receipt of the PIN envelope.

h. Upon confirmation that the user received the PIN envelope, the appropriate dSO will activate the smartcard. If the PIN envelope is lost or tampered with, the dSOs should unassign the card. The user should be informed to return the card **Certified Mail - Return Receipt Requested**. Return this card to the cSOs for reinitialization.

4.1.5.8 Deactivate Smartcards.

a. Smartcards do not have an infinite lifetime. Smartcards may be lost or stolen, PINs may be compromised, or smartcard users may retire, transfer, or quit. The "DSO DEACTIVATE SMARTCARD SCREEN" allows dSOs to deactivate expired smartcards or smartcards for users who retire, transfer, or leave the organization.

b. All cards available to be deactivated will be displayed. The dSOs may query on any of the fields in order to query up the card to be deactivated. When menu option "10" is selected, the "**DSO DEACTIVATE SMARTCARD SCREEN**" will be displayed.

c. When the correct smartcard to be deactivated is displayed, the dSOs must enter a 'Y' in the DEAC? block and then depress <End>.

d. The dSOs must require the user to turn in the card before deactivation.

e. A LOG SHEET OF DEACTIVATED SMARTCARDS will be signed by the user.

f. This option is to deactivate cards which have not been lost or stolen. Only smartcards with a status value of "C", which indicates an active smartcard may be deactivated.

g. Care should be taken when deactivating smartcards for they cannot be reactivated.

4.1.5.9 Lost Smartcards.

a. This option is to deactivate cards which have been lost or stolen. The user must notify the DSO immediately if a card is lost or stolen.

b. When menu option "11" is selected, the '**DSO LOST SMARTCARD SCREEN**" will be displayed. All cards available to be deactivated will be displayed. The dSOs may query on any of the fields in order to query up the card to be deactivated.

c. Enter 'Y' by the requesting user/card number and the date the card was lost and then depress the <End> key.

d. A LOG SHEET OF LOST SMARTCARDS will be maintained by the dSOs. Smartcard users will be required to sign the log sheet for lost smartcards.

e. Signatures generated by the user before the lost card date may still be verified.

4.1.5.10 Unlock User Smartcard.

a. The normal operation of Electronic Signature in CEFMS requires that an SA and a User be logged on with their respective smartcards to electronically sign documents. The User smartcard must remain in the smartcard reader until a prompt is displayed indicating that it is safe to remove the User smartcard. If the User smartcard is removed before the prompt saying it is safe to do so, the User smartcard will be "locked" and unusable until unlocked. This screen is used to unlock User smartcards.

b. Before unlocking a Smartcard, the dSOs should verify that the person presenting the card is, in fact, the owner of the card. The user should present a valid driver's license or civilian identification. Refer to paragraph "View Smartcard Information" for Smartcard holder verification procedures. Do not unlock the card if the person presenting the card is not the authorized user of that card.

c. When menu option "12" is selected, the '**UNLOCK SMARTCARD SCREEN**" will be displayed. A prompt is displayed asking the dSOs to remove the dSO2 or dSOb2 smartcard from the smartcard reader. The smartcard**must** be removed. After the smartcard is removed, a prompt requesting that the smartcard to be unlocked be inserted into the smartcard reader be will be displayed. The smartcard to be unlocked should be inserted into the smartcard reader. A prompt will be displayed indicating that the smartcard is being unlocked. After the smartcard is unlocked, a prompt will be displayed requesting that the newly unlocked smartcard be removed from the smartcard reader. When the smartcard is removed the dSO Functions Menu will be re-displayed. This process must be repeated to unlock another smartcard.

4.1.5.11 Order Smartcards.

a. As each COE District brings CEFMS online, the dSOs will be supplied with beginning inventories of smartcards and their associated PIN envelopes. These inventories will require re-supply at some point. When additional smartcard supplies are needed, dSOs will order via this menu selection.

b. When menu option "13" is selected, the '**SMARTCARD ORDERING SCREEN**" will be displayed with two enterable fields.

c. The dSOs will enter the numeric amount of additional User and SA cards required in their respective fields on the screen. To commit the request and cause the request to be transmitted to the Central Key Translation Facility, depress the <End> key. In addition to the menu option for ordering smartcards, the Request for Electronic Signature (Smartcard Initialization) Form provided in Appendix B, must be completed when mailing cards to cSOs for initialization.

d. The requested smartcards and their associated PIN envelopes will be mailed to the dSOs. It should be noted that dSO1 and dSOb1 will have access to the User smartcards and the SA PIN envelopes. The dSO2 and dSOb2 will have access to SA smartcards and User PIN envelopes.

e. All unissued smartcards and PIN envelopes must be stored according to conditions discussed in paragraph 4.2.

4.1.5.12 Key Translation Center/ORACLE SID Setup.

a. This function should be accessed to initially define and then to redefine as necessary, the following information:

ORACLE SID
PRIMARY TRANSLATE KEYS HOST NAME
SECONDARY TRANSLATE KEYS HOST NAME
CURRENT VERSION NUMBER OF ESIGISR
DOWNLOAD PATH TO ESIGISR

b. When menu option "14" is selected, the "KEY TRANSLATION CENTER/ORACLE SID SETUP" screen will clear and the '**KEY TRANSLATION CENTER/ORACLE SID SETUP**" screen will be displayed. Simply use the cursor keys to move to the desired field and then enter the desired information. When finished, depress the <END> key to commit the new information and <F10> to exit.

4.1.5.13 Key Translation Center/Card Request Setup.

a. This function should be accessed to define FOA Code, Oracle SID, and Card Request Counter value. When menu option "15" is selected, the "**KEY TRANSLATION CENTER/CARD REQUEST SETUP**" screen is displayed.

b. The card request counter value must always be set to 0 initially.

c. To enter a new record depress <F9>. The cursor will be positioned at the FOA code field of the new record. Enter the FOA CODE and depress <ENTER>, the cursor will advance to the ORACLE SID field. Enter the SID value to be associated with the FOA CODE and depress <ENTER>. The cursor will be positioned at the CARD REQUEST COUNTER field. Enter a 0, then <END> to commit. Depress <F10> to exit the form and return to the previous screen.

4.1.6 Menu Selection 8 - Execute dSO Startup Utility.

a. This function is accessed from the Electronic Signature Menu. This function should be accessed once, and only once, to assign and activate the initial two dSO smartcards at a site.

b. When invoked, dS01 and dS02 should be present with their dSO smartcards. Each dSO will be requested to insert their smartcard into the smartcard reader and enter their associated PINs. Once this function is complete, the participating dSO smartcards will be activated and ready for normal use.

c. All future dSO card assignments for the database should be done using the screens required to issue user cards.

4.2 Storage of Smartcards and PIN Envelopes.

a. Generated electronic signature user cards and PINs received by the District Security Officers (dSO1 and dSO2) should be separately maintained and secured in a GSA-approved security container with an approved built-in, three-position, dial-type changeable combination lock, suitable for the storage of secret and confidential information. A safe-type filing cabinet may be used if each drawer has a combination lock or if an electronic lock which requires two people to open has been installed. A Security Container Check Sheet, Standard Form 702, must be placed on the container to record each time the container is opened and closed, by whom, and a closing check. Please refer to the U.S. Department of Commerce National Security Information Manual, DAO 207-2, Chapter 8 for above guidance. Combinations should be changed in accordance with DAO 207-2, Chapter 8, paragraph 805.

b. PINs and cards must be stored in GSA approved security containers at all times unless under physical control of the responsible dSO. The cards and PINs should only be accessible to the responsible dSO or his backup.

c. DSO1/dSOb1 will store User smartcards and SA PIN envelopes in one container and will be the only authorized key holders.

d. DSO2/dSOb2 will store SA smartcards and User PIN envelopes in the other container and will be the only authorized key holders.

e. Contact the Security Officer for information regarding security containers or to report known or suspected violations involving smartcards or PINs.

f. Once issued, the smartcard holder is responsible for their smartcard and PIN.

4.3 Error Messages.

a. Smartcard processing may result in errors. The following error codes and messages are listed to aid in the diagnosis of error conditions.

ERROR CODE	EXPLANATION OF ERROR
0	ElecSig: Success
1	Cannot get terminal characteristics
2	Cannot stat terminal driver
3	Cannot find interface program
4	Transmit of data failed
5	Unspecified ESIGMGR failure
6	Cannot set TTY to raw model
7	Cannot change TTY model
8	Network load to high, can't communicate with / RCV communication timeout
9	Cannot find interface program
10	SA logon terminated voluntarily
11	User card is locked, contact security office
12	Translate keys not available
13	SA logon failed
14	User logon failed
15	No response from PC
16	Error getting host name
20	Security adaptor missing
21	Data integrity failed, contact document originator
22	Security breach
23	User card removed
24	ESIGMGR not responding, esig impossible
25	Service failed
26	Host failed

27	Proto failed
28	Read socket create
29	Read socket bind
30	Read socket name
31	Read socket listen
32	Write socket create
33	Write socket connect
34	Write failed
35	Request for new cards failed
36	Inactive user card used
37	Inactive SA card used
39	Unauthorized command attempted
60	Header MAC received does not match computed
90	Password must be at least 8 chars
91	Password entered incorrectly
92	SO logon voluntarily terminated
93	Esig changed
94	Cannot open connection
95	ESIGISR not loaded
97	No free key record in card
98	Key ID not found
99	No free key entry in adaptor
100	Key record's card address is zero
101	Invalid active key number
102	Key parity error
103	Invalid key type
104	Key management not initialized
105	Invalid card header
106	Invalid function for link model
107	Privilege violation
108	Unused key record in card
109	Invalid key record in card
110	Suspended key record in card
111	Key entry in use
112	No such key entry
113	Key entry not in use
114	No key encrypting key active
115	Key with given ID already in key store
116	Invalid key type for key function given
117	Key already active
118	Key entry checksum failure
119	Invalid password
120	Attempt to decrement key counter

121	Incompatible key sizes
123	Key XOR violation
124	Key encryption violation
125	Key is discontinued
126	Key checkword failure
127	Link authentication failure
128	OU mac after deactivation date
129	OU mac after lost date
130	OS mac after deactivation date
131	OS mac after lost date
132	RU mac after deactivation date
133	RU mac after lost date
134	RS mac after deactivation date
135	RS mac after lost date
150	Field format error
151	Nested delimiters
152	Unmatched delimiters
153	Duplicate MID, MAC, or date field
154	No date field
155	No MAC field
156	No MID field
157	Accept failed
158	Read failed
159	SO not logged in
160	No data to MAC in storage
161	No MAC to verify (esig not mandatory)
162	Initialize CEFMS failed (esig not mandatory)
163	No MAC to verify (esig mandatory)
164	Initialize CEFMS failed (esig mandatory)
165	DSO1 logon failed
166	DSO2 logon failed
167	Must use ESIGMGR, not VCOM menu - emulation flag error
220	Dirty line
221	Checksum failed
225	No such card
226	Card already active
227	Cryptoperiod has expired
228	User cryptoperiod has expired
229	SA cryptoperiod has expired
230	Orig User cryptoperiod has expired
231	Orig SA cryptoperiod has expired
234	Bad Org SAID
235	Bad Org UserID

236	Bad RCV SAID
237	Bad RCV UserID
238	Counter for this instance is not stored at.KMS
239	Counter for this instance is out of sync with KMS counter
240	Could not connect to ORACLE to retrieve counter
240	User logon terminated voluntarily
241	Could not SELECT counter field from FOA -UNIQUE table
246	User pressed "skip" key
247	User pressed "quit" key
248	Your ElecSig driver is the wrong version. Contact system administrator
249	dSO2 card not in receptacle
251	Oracle error - 1002, 1403 nothing return from select (treat this as a warning)
255	Driver initialization failed, no elecsig capability
255	Cannot verify, document was not electronically signed
999	Unknown error

APPENDIX A

DSO ACKNOWLEDGEMENT FORM

I certify that I have read and understand my responsibilities as a District Security Officer (dSO) and that I am a Government employee.

PRINTED OR TYPED NAME	SIGNATURE

OFFICE SYMBOL	EXTENSION	DATE

APPENDIX B

REQUEST FOR ELECTRONIC SIGNATURE FORM (Smartcard Initialization)

REQUEST FOR ELECTRONIC SIGNATURE FORM
(Smartcard Initialization)

REQUESTING SITE: _____

NAME (dSO1): _____ **Phone No.: ( ) -** _____

MAILING ADDRESS (dSO1): _____

_____

NAME (dSO2): _____ **Phone No.: ( ) -** _____

MAILING ADDRESS (dSO2): _____

_____

CARD REQUESTS:

NO. OF USER CARDS: _____

NO. OF SA CARDS: _____

NO. OF dSO CARDS: _____

SIGNATURES:

dSO1: _____ **dSO2:** _____

a. Card Serial No.	b. Date of Initialization	c. Destination dSO1/dSO2

SIGNATURES:

cSO1: _____ cSO2: _____